# Security in electronic communication: digital signatures and encryption

1997/2235(COS) - 08/10/1997 - Non-legislative basic document

OBJECTIVE: defining a European policy to ensure security and trust in electronic communication and digital signatures. SUBSTANCE: the Commission's document indicates that, if nothing is done soon, the development of electronic commerce could be hampered by the insecurities typical to open networks such as Internet. Messages may be intercepted and manipulated, the validity of documents can be denied and personal data can be illicitly connected. Cryptographic technologies for instance, digital signatures and encryption may provide an essential tool for security and trust on open networks. Several Member States have already announced their intention of introducing specific regulations in this area and some of have already done so. However, divergent practices (or the absence of regulation) could constitute a serious barrier to electronic commerce. Accordingly, the objective of the Commission communication is to develop a European policy in this area. Legislative proposals could be presented as soon as 1998 in the light of responses to proposals contained in this communication. In particular, the Commission considers that a Community strategy should contain the following elements: 1) In the field of digital signatures: - laying down common legal requirements for certifying authorities (CAs) so as to create a framework for the mutual recognition of certificates issued by CAs; - establishing equivalent legal recognition for digital and conventional signatures; - encouraging international cooperation to create a suitable framework for worldwide electronic commerce and in particular establish common technical standards and commence the mutual recognition of certificates. 2) With regard to encryption: the Commission considers that encryption is frequently the only effective means of protecting data and communications on open networks. As far as the national authorities are concerned the large-scale use of encrypted communication could diminish their capacity to fight against organized crime. In this respect, the Treaty fully respects the competences of the Member States in the field of national security. However, national restrictions should not hamper electronic commerce and infringe Community law. The Commission will therefore examine national restrictions in the light of existing provisions concerning freedom of movement, the principle of proportionality, Directive 83/189/EEC concerning standards and technical regulations and Directive 95/46 /EC on the protection of personal data. Additional measures could be envisaged with a view to strengthening the control of encryption (for example adjustment of Regulation (EC) No 3381/94 on the control of exports of dual-use products, improving the cooperation between police forces and the conclusion of international agreements). Finally, the following accompanying measures could be envisaged as of 1998: 1) encouraging the industry and international standardization bodies to develop their interoperable technical and infrastructural standards for digital signatures and encryption; 2) proposal for a Council and Parliament decision for an INFOSEC II programme (development of overall strategies for the security of electronic communications); 3) launching of new projects in the framework of the fifth RTD framework programme in the field of electronic communications; 4) encouraging the utilization of digital signatures and encryption by the Community's and public authorities; 5) creation of a European Internet forum as a means of information and exchange; 6) organization of an international hearing of experts on digital signatures and encryption.